AMENDMENTS TO THE SPECIFICATION:

Please amend the third full paragraph on page 1 as follows:

In remote operation of the contents and configuration of services which a storage system provides to users, it is necessary to provide a means for overwriting a configuration information database of the storage system. Conventional means for accessing data includes an access method by using a general purpose simple network management protocol (SNMP), an access method by creating a specific protocol and defining a specific interface for accessing a database to make an application program access the database by using the interface, or other access methods. Such an application program uses a program distributed and installed in each manager in advance. The program is allowed to be used only by those ~~certified~~ authenticated by an ID and password. This ~~certification~~ authentication mechanism is generally implemented beforehand in the application program.

Please amend the second full paragraph on page 2 as follows:

A security function such as ~~certification~~ authentication is required to be implemented beforehand in an application program, which may increase illegal accesses. Management by using an SNMP protocol is associated with disadvantages in terms of performance and security.

Please amend the paragraph bridging pages 3 and 4 as follows:

According to one aspect of the present invention, there is provided a storage management system comprising: a management object for controlling a request from a manager which manages a data file to be accessed by a user, the management object ~~certifying~~ authenticating a second manager ID and a second manager password received from the manager, in accordance with a first ID and a first password stored beforehand; and interfaces to be created by the

management object when the ~~certification~~ authentication of the second manager password and the second password by the management object succeeds, and to be expired after a predetermined time, the interfaces permitting an access from the ~~certified~~ authenticated manager.

Please amend the second full paragraph on page 4 as follows:

This interface is dynamically created or loaded in a service processor in response to a request from a manager accessing via a network such as the Internet and an intranet, and expired when a log-out from a manager program is received. A use condition of the interface depends upon ~~certification~~ authentication of a manager ID and password. In order to identify a manager to which the use of the interface is permitted or prohibited, a manager information file is provided which may store a manager ID and password, a usable interface method (function) group, a use period, and most recent log-in/log-out times, respectively for each manager.

Please amend the first full paragraph on page 6 as follows:

A storage system of this embodiment has: a storage device 100 such as a disc storing a large capacity of data for inbound users or storage users connected via an interface 99; and a management mechanism for managing the large capacity of data in response to an instruction from a manager 109 via a network 500 as shown in Fig. 1.

Please amend the paragraph bridging pages 7 and 8 as follows:

The RMI interface object 107 is software which can exist by being dynamically created when necessary (it is possible to design in such a manner that the RMI interface object 107 is automatically expired if a non-access time of the RMI interface object becomes equal to or longer than a predetermined time). If this object 107 does not exist, access to the storage

configuration information file 106 is permitted not at all. While this object 107 exists, the storage configuration information file 106 can be accessed from an external JVM computer. In this case, it is necessary to know an RMI address of the RMI interface object 107, and if the RMI address is not known, the storage configuration information file 106 cannot be accessed. When the RMI interface object 107 is dynamically created, the RMI address is randomly generated. By using this randomly assigned RMI address as ~~a certification~~ an authentication key 107a and giving this ~~certification~~ authentication key 107a to only the manager permitted to use the RMI interface 108, a safer RMI interface 108 can be implemented.

Please amend the first full paragraph on page 8 as follows:

While a plurality of managers access, a corresponding plurality of interfaces run in the service processor as software responding to each secret key or ~~certification~~ authentication key.

Please amend the second full paragraph on page 8 as follows:

When the storage manager program 102 uses the RMI interface 108 via the network 500, the program 102 requests the RIM server program called the RMI management object 105 to create the RMI interface object 107, and after the RMI interface object 107 is created, the program 102 uses the RMI interface method or function. In this case, the RMI address as a key for accessing the RMI interface 108 is acquired from the RMI management object 105. However, this RMI address cannot be acquired unless the management object 105 is subjected to ~~certification~~ authentication by the manager information file 104. For example, ~~certification~~ authentication techniques of using a manager ID and password may be used. Namely, the manager information file 104 storing a list of manager ID's and passwords is prepared to perform

~~certification~~ authentication through comparison with information transmitted from the storage manager program. Therefore, the manager program connected to this interface cannot use this interface unless the ~~certification~~ authentication is made by the manager ID and password. A safer interface system can therefore be implemented.

Please amend the first full paragraph on page 9 as follows:

With a conventional method of guaranteeing security by ~~certification~~ authentication by the manager program of the manager 109, if a program miss or a security hole of the manager program is found, there is a fear that the storage configuration information file is accessed via this application program. In addition, if a third party creates an illegal access program for accessing the interface, the interface may be stopped or is required to be created again.

Please amend the paragraph bridging pages 9 and 10 as follows:

As illustratively shown in Fig. 2, the manager information file 104 to be used for ~~certification~~ authentication by the RMI management object may store for each registered manager: information such as a manager ID 104a and a password 104b; a file name 104c of a permission period information file 104-1 storing a permission period; a file name 104d of a permission function information file 104-2 storing information on a use permission function group; a most recent log-out time 104e; and the like.

Please amend the second full paragraph on page 10 as follows:

The manager acquires information necessary for ~~certification~~ authentication such as the manager ID 104a and password 104b from the ~~certification~~ authentication interface built in the

storage manager program 102, and transmits the acquired information to the RMI management object 105 (Step 203).

Please amend the paragraph bridging pages 10 and 11 as follows:

In accordance with the procedure as will be illustratively described with reference to Fig. 4, the RMI management object 105 executes ~~a certification~~ an authentication process for the manager, and if the ~~certification~~ authentication succeeds (Step 204), creates the ~~certification~~ authentication key 107a (RMI object address) necessary for RMI use permission, and creates the RMI interface object 107 corresponding to the ~~certification~~ authentication key 107a (Step 205).

Please amend the first full paragraph on page 11 as follows:

The RMI management object 105 transmits the ~~certification~~ authentication key 107a to the storage manager program 102 running on the WWW browser of the manager 109 (Step 206).

Please amend the second full paragraph on page 11 as follows:

The storage manager program 102 acquires the RMI object address from the received ~~certification~~ authentication key 107a to thereafter access the RMI interface 108 of the RMI interface object 107 and perform a desired system management work and the like such as reference and alteration of the configuration information of the storage system 101 (Step 207).

Please amend the fourth full paragraph on page 11 as follows:

If the ~~certification~~ authentication fails at Step 204 (in the case of the illegal accessor 110), the log-out is performed forcibly (Step 208).

Please amend the fifth full paragraph on page 11 as follows:

With reference to the flow chart shown in Fig. 4, the ~~certification~~ authentication process to be executed by the RMI management object 105 in the storage system 101 of this embodiment will be described more in detail.

Please amend the paragraph bridging pages 11 and 12 as follows:

First, ~~certification~~ authentication is made by comparing the manager ID and password transmitted from the manager side with the contents registered in the manager information file 104 (Step 401) and reference is made to the end time (log-out time 104e) of the RMI interface object most recently accessed by the manager (Step 402). A non-use time duration is calculated from the log-out time 104e and a current time, and if the non-use time duration exceeds a threshold value (Step 403), the RMI interface object is not created but a forcible log-out of the manager is executed (Step 410). In this manner, it is possible not to give a use permission to the manager in a long non-use time duration state.

Please amend the paragraph bridging pages 12 and 13 as follows:

If the ~~judgement~~ judgment Step 405 is asserted, first the ~~certification~~ authentication key 107a is created (Step 406). Then, as illustratively shown in Fig. 5, the function group to be permitted to use is discriminated from the use permission function information file 104-2 by using the list in the manager information file 104, and the RMI interface object 107 is created in accordance with the information of the permitted function group and ~~certification~~ authentication key 107a (Step 407). The RMI interface object 107 has therein the permission flag 107b for each

function 107c. Each function 107c can be used only when the use permission flag 107b is valid and in addition since the RMI interface object address is dependent upon the ~~certification~~ authentication key 107a, the manager not having the ~~certification~~ authentication key 107a cannot use the RMI interface object.

Please amend the first full paragraph on page 13 as follows:

Thereafter, the management object 105 transmits the ~~certification~~ authentication key 107a to the storage manager program in the browser 109 (Step 408).

Please amend the second full paragraph on page 13 as follows:

In accordance with the ~~certification~~ authentication key 107a received from the RMI interface object 107, the storage manager program of the manager obtains the RMI address so that the RMI interface 108 can be accessed (Step 409).

Please amend the second full paragraph on page 15 as follows:

Manager interfaces such as the RMI interface object 107 and RMI interface 108 for management control or the like of the storage system do not exist before ~~certification~~ authentication, and exist only after the ~~certification~~ authentication. Since the interfaces cannot exist without the ~~certification~~ authentication, a management control interface system for the storage system 101 can be implemented with high security.

Please amend the first full paragraph on page 16 as follows:

The management control software specific to a manager to be connected to the interface for management control or the like of the storage system 101 is not necessary to have a ~~certification~~ authentication function. This provides the effects of preventing security from being lowered by giving the ~~certification~~ authentication function to specific management control software.